12 FAM 390
SECURITY EQUIPMENT AND MAINTENANCE

(CT:DS-201; 01-08-2014)
(Office of Origin: DS/C)

12 FAM 391 SCOPE AND AUTHORITY

12 FAM 391.1 Purpose

(CT:DS-201; 01-08-2014)

The Department provides security for U.S. Government diplomatic operations, including the protection of all U.S. Government personnel on official duty abroad under chief of mission (COM) authority. The Department also develops and implements technical and physical security programs and maintains and repairs security equipment installed at posts abroad. This policy does not address alarm or access control systems domestically or those related to sensitive compartmented information facilities (SCIFs) at posts abroad.

12 FAM 391.2 Applicability

(CT:DS-174; 03-15-2012)

These regulations apply to all office facilities at U.S. posts abroad that have equipment as described in this subchapter. Posts must only use the Facility Security Engineering Division (DS/ST/FSE)-approved locking devices and the Physical Security Division (DS/PSP/PSD)-approved physical security equipment, in the physical security systems of these facilities.

12 FAM 391.3 Authorities

(CT:DS-201; 01-08-2014)

a. The Omnibus Diplomatic Security and Antiterrorism Act of 1986 (Public Law 99-399; 22 U.S.C. 4801, et seq. (1986)), as amended.

b. 12 FAH-5 H-020 Concepts and Philosophy.

c. 12 FAH-6 H-632 Intrusion Detection Alarm Standards.

d. The Bureau of Diplomatic Security Classification Guide for Design and

Construction of Overseas Facilities.

e. 3 FAM 4370 Disciplinary Action

12 FAM 392 SPECIAL PROTECTIVE EQUIPMENT

(CT:DS-174; 03-15-2012)

Security standards for issuing and controlling Department special protective equipment (SPE) are codified in the 12 FAH-6, Overseas Security Policy Board (OSPB) Security Standards and Policy Handbook. You must address all requests for SPE to the Defensive Equipment and Armored Vehicles Division (DS/PSP/DEAV).

12 FAM 393 PHYSICAL AND TECHNICAL SECURITY EQUIPMENT PROGRAM

(CT:DS-174; 03-15-2012)

Diplomatic Security (DS) and the Bureau of Overseas Buildings Operations (OBO) developed the Security Equipment Responsibilities Matrix, which lists the organizations responsible for physical security equipment installation, maintenance, and repair at U.S. posts abroad. The matrix is available on the Construction, Facility, and Security Management (OBO/CFSM) and the Office of Security Technology (DS/C/ST) Web sites.

12 FAM 394 PHYSICAL SECURITY INTRUSION DETECTION SYSTEM AND AUTOMATED ACCESS CONTROL SYSTEM INFORMATION AND DATA

12 FAM 394.1 Scope and Applicability

(CT:DS-201; 01-08-2014)

Physical security intrusion detection systems (IDSs) and automated access control systems (AACSs) are elements of the in-depth security infrastructure protecting Department personnel and resources. The information about those systems, as well as passwords and personal identification numbers (PINs) used to access and manipulate them, requires protection to ensure their operational effectiveness. This policy describes the controls and levels

of protection required for information and data about Department IDS and AACS installed at posts abroad.

12 FAM 394.2 AACS and IDS Overview

(CT:DS-201; 01-08-2014)

The 12 FAH-5 describes the philosophy of tiered defense. AACS and IDS are two defensive measures that contribute to the protection of Department personnel and resources. While the measures may combine to protect the highest level of classified information, the classification of individual protective components varies from Unclassified to Secret. The Security Classification Guide for Design and Construction of Overseas Facilities describes classification requirements of design and operational aspects of these systems. This *subchapter addresses* the protection of IDS and AACS data and information not addressed in the Classification Guide. Refer questions about perceived conflicts between this *subchapter* and the Classification Guide to DS/C/ST.

12 FAM 394.3 IDS and AACS Control Equipment

(CT:DS-201; 01-08-2014)

IDS control equipment and associated sensor cables protecting an area must reside within the protected space or in a space protected at a higher level. For IDS protecting a controlled access area (CAA), the control panel and associated sensor cables must reside within a space designated for storage at the highest level of classification that the IDS is protecting. Additionally, any data transmitted outside the CAA must be protected with DS-approved encryption or a DS-approved distribution system.

12 FAM 394.4 IDS and AACS PINs Internal Data

(CT:DS-201; 01-08-2014)

a. Installation per 12 FAM 394.3 provides a level of protection for the system data, but the typical IDS or AACS control equipment enclosure does not qualify as safe file containers for storage of classified information.

b. While the PINs, passwords, and programming data are not classified, those managing, handling, and using the data must protect it on a strict need-to-know basis to limit availability and ensure the effectiveness of the systems. Anyone entrusted with such information must not divulge or expose it to others. Users should memorize PINs and passwords and take positive measures to protect recorded information. Carrying PINs and passwords for personal convenience, such as in *your* wallet or purse,

is strictly prohibited.

c. The RSO and Engineering Services Center (ESC)/Engineering Services Office (ESO) personnel must put in place safeguards such as maintaining and reviewing IDS audit logs, removing unused PINs, and securely storing PINs to protect against compromise. Hardcopy of PIN codes and other IDS-specific data must be stored in a General Services Administration (GSA)-approved safe controlled and used only by cleared American personnel with a "need-to-know." Alternatively, IDS data may be stored on a stand-alone computer or on a protected network (like the Security Management System Enterprise Network (SMSeNet)), as long as the PC is both physically protected (in either a limited access area (LAA) or a CAA) and logically secured through user authentication. Do not store IDS or AACS data on an OpenNet or ClassNet workstation.

d. Those security personnel responsible for assigning IDS and AACS PINs and passwords to users must document PIN and password distribution. The receiving individuals must acknowledge receipt of the information and their responsibility to protect it by not divulging it to anyone. The 12 FAM Exhibit 394 provides a suggested format to document the process.

12 FAM 394.5 Authority to Secure and Penalty for Misuse

(CT:DS-201; 01-08-2014)

Failure to provide the prescribed protection for PINs, passwords, and other sensitive IDS or AACS information may result in disciplinary action (see 3 FAM 4370). Penalties for criminal misuse or subversion of this information for personal gain will be dealt *with* in accordance with 18 U.S.C. 641.

12 FAM 395 THROUGH 399 UNASSIGNED

12 FAM EXHIBIT 394
SAMPLE FORMAT FOR RECEIPT/SECURITY ACKNOWLEDGEMENT OF IDS AND AACS PINS AND PASSWORDS

(CT:DS-201; 01-08-2014)

(Prepare on Department or Post Letterhead Stationery)

I hereby acknowledge receipt of all personal identification numbers (PINs) and passwords listed below and understand that:

(1) I am responsible for the protection of my PINs and passwords;

(2) I will comply with all applicable security standards; and

(3) I will not divulge my PINs or my passwords.

(4) Failure to provide the prescribed protection for PINs, passwords, and other sensitive IDS or AACS information may result in disciplinary action (see 3 FAM 4370). Penalties for criminal misuse or subversion of this information for personal gain will be handled in accordance with 18 U.S.C. § 641.

I further understand that I must immediately report to the Regional Security Office (RSO) if I have reason to suspect that one or more of my PINs or passwords have been compromised.

SYSTEM **PIN/Password**

_____

_____

_____

Signature _____ Date _____

Printed Name _____

Office/Post _____ Work Phone _____

Security Manager's Signature _____ Date _____